Cryptographic Protocol Analysis via Strand Spaces

Joshua D. Guttman

Jonathan C. Herzog

F. Javier Thayer

September 2000

MITRE

Outline of Introductory Talk

To study the Dolev-Yao problem

- What is a cryptographic protocol?
- What is the environment in which it is used?

- Identify security goals for cryptographic protocols
- Model crypto protocols and their security goals
- Show how to use analysis method: How to
  - Discover flaws
  - Prove no flaws exist
  - Find if combining protocols creates flaws
  - How to design protocols without flaws
- Justify analysis method

The Problem

- What is a cryptographic protocol?
  - Short, convention-bound sequence of messages
  - Uses cryptography
  - Aims at authentication, secret key distribution, etc.
- Cryptographic protocols are often wrong
  - Active attacker can subvert goals
  - May fail even if cryptography ideal
  - Hard to predict which protocols achieve what goals
- Cryptographic protocols are important

– Central to security
for communications, networks,
distributed systems, e-commerce

The Dolev-Yao Problem

- Given a protocol, and assuming all cryptography perfect, find
  - What secrecy properties
  - What authentication properties

  the protocol achieves
- Find counterexamples to other properties
  - Unintended services useful
- What does perfect cryptography mean?
  - No collisions
  - Need key to make encrypted value
  - Need key to recover plaintext

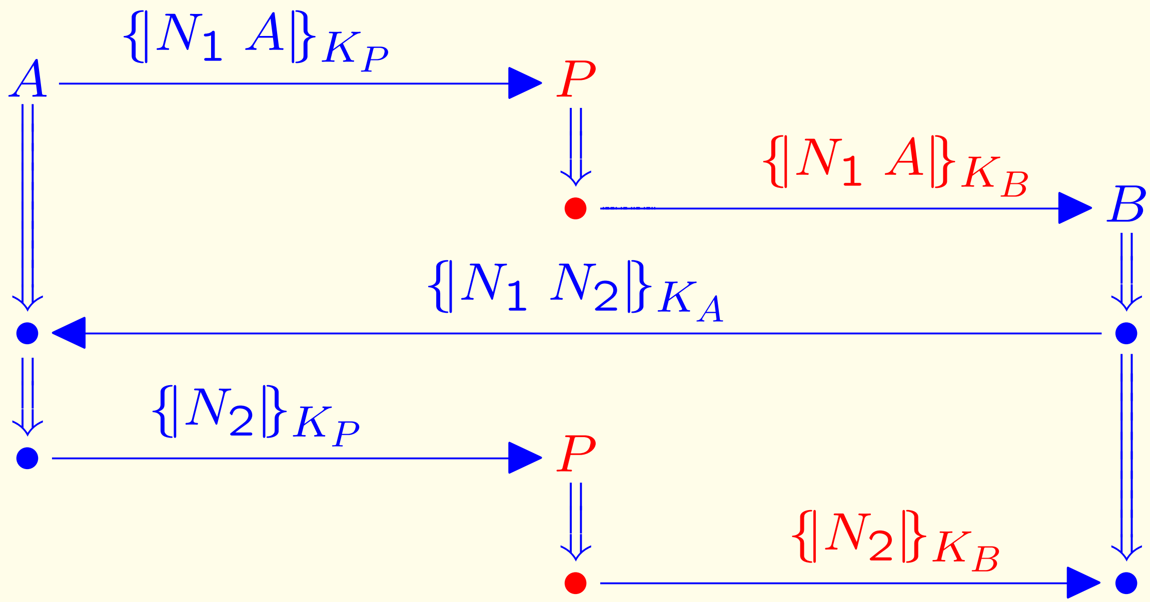
Needham-Schroeder Protocol, 1978

$$\begin{tikzcd}
A \arrow[r, "\{\!|N_1\ A|\!\}_{K_B}"] \arrow[d, Rightarrow] & {} & {} \arrow[r, "\{\!|N_1\ A|\!\}_{K_B}"] & B \arrow[d, Rightarrow] \\
\bullet \arrow[d, Rightarrow] & {} \arrow[l, "\{\!|N_1\ N_2|\!\}_{K_A}"'] & {} & \bullet \arrow[l, "\{\!|N_1\ N_2|\!\}_{K_A}"'] \arrow[d, Rightarrow] \\
\bullet \arrow[r, "\{\!|N_2|\!\}_{K_B}"] & {} & {} \arrow[r, "\{\!|N_2|\!\}_{K_B}"] & \bullet
\end{tikzcd}$$

Needham-Schroeder: Intended Run

$$\begin{tikzcd}
A \arrow[r, "\{\!|N_1\ A|\!\}_{K_B}"] \arrow[d, Rightarrow] & B \arrow[d, Rightarrow] \\
\bullet \arrow[d, Rightarrow] & \bullet \arrow[l, "\{\!|N_1\ N_2|\!\}_{K_A}"'] \arrow[d, Rightarrow] \\
\bullet \arrow[r, "\{\!|N_2|\!\}_{K_B}"] & \bullet
\end{tikzcd}$$

Needham-Schroeder: Undesirable Run



Due to Gavin Lowe (1995)

Diagnosis of a Failure

- Who was duped?
  - Not A: Meant to share N_1, N_2 with P
  - B: Thinks he shares N_1, N_2 only with A
    - Secrecy failed: P knows values
    - Authentication failed: A had no run with B
- How? A offered P a service:
  - Gave P nonce N_1
  - Promised to translate $\{\!|N_1, N|\!\}_{K_A}$ to $\{\!|N|\!\}_{K_P}$
- An "unintended service"
  - Attacker needs to compute some value
    - N_2 in this case
  - But legitimate party creates such a value

History of Problem, I: Dolev-Yao, 1981

- Separated protocol problem from cryptographic correctness
  - Idealize cryptography
  - Discover attacks due to protocol structure
- Separated behavior into
  - Regular participants (assumed predictable)
  - Active penetrator
- Identified powers of penetrator
  - Controls communication
  - May exploit multiple sessions
  - May apply public keys, some private keys

- Focused on secrecy goals

History, II: Logics of Belief

- Regard messages as "utterances," protocol goals as justified beliefs
  - Problem: what utterance does a message convey?
- Inaugurated in great paper, Burrows-Abadi-Needham, 1989
- Semantical issues were subtle
  - Soundness theorems OK
  - Operational meaning of model theory tricky
  - Playground for the logically over-privileged?

History, III: Search

- Regard protocol as state machine
  - Find sequence of events
    with bad outcome
  - May work backwards
    (more focused, symbolic)
    or forwards
    (faster state examination)
- Protocol search tools
  - Interrogator (mid 80s)
  - NRL Protocol Analyzer (early 90s)
    also allowed pruning via lemmas
- General-purpose model checking

- Process algebras
  (CSP/FDR: mid 90s)
- Hardware verification tools

Our Approach: A Proof Method

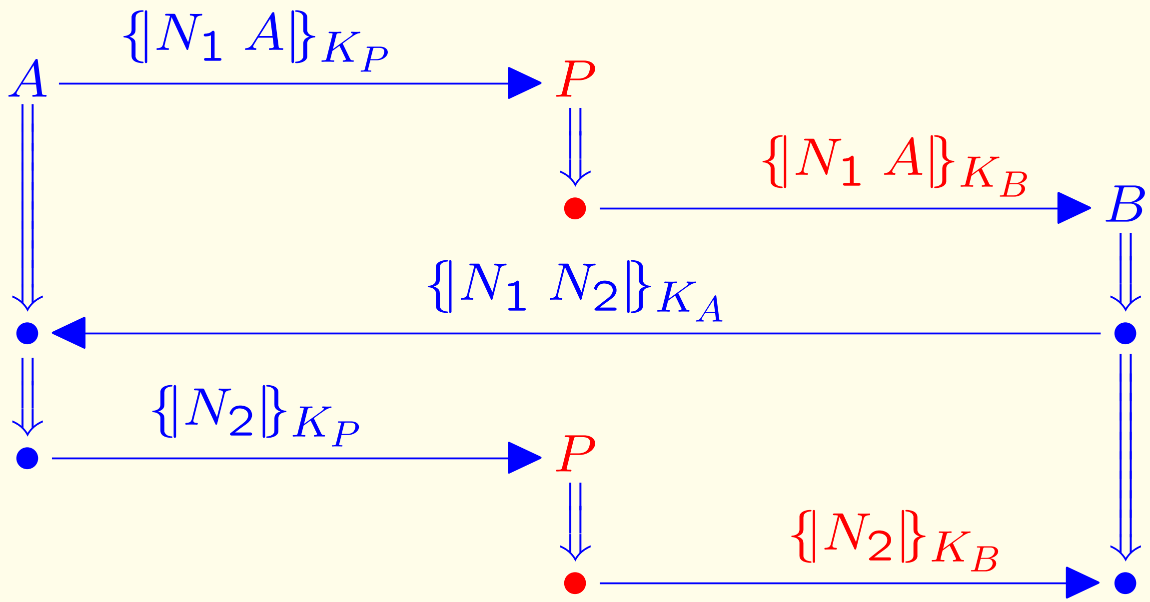
- History:
  - Dolev-Even-Karp (1982)
  - Woo-Lam (early 90s), Bolignano (mid 90s)
  - Schneider, Paulson: CSFW, June 97
  - Strand spaces: November 97
- Strand spaces: Simple model to express
  - Protocol behavior
  - Penetrator powers
  - Protocol goals (authentication, secrecy)
- Methods to prove protocol meets goals

- Discover exact hypotheses for goal
- Unprovable goals suggest attacks
- General theorems about
  classes of protocol

Modeling Cryptographic Protocols via Strand Spaces

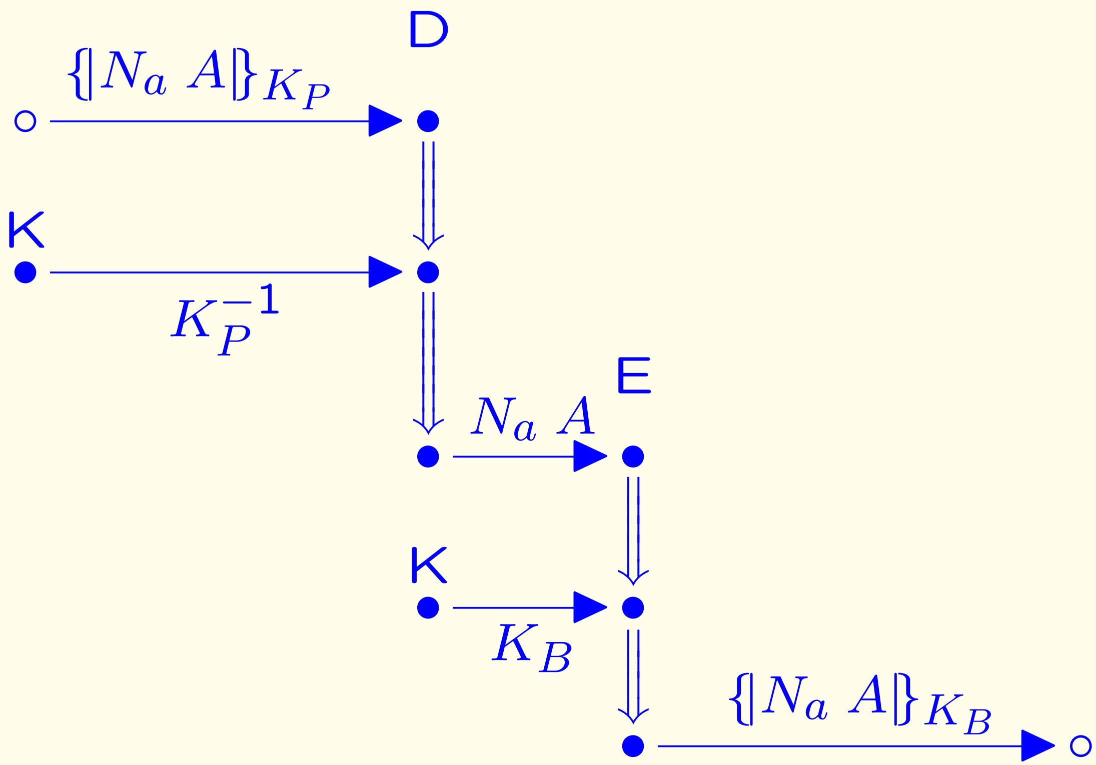
MITRE

Needham-Schroeder: Undesirable Run

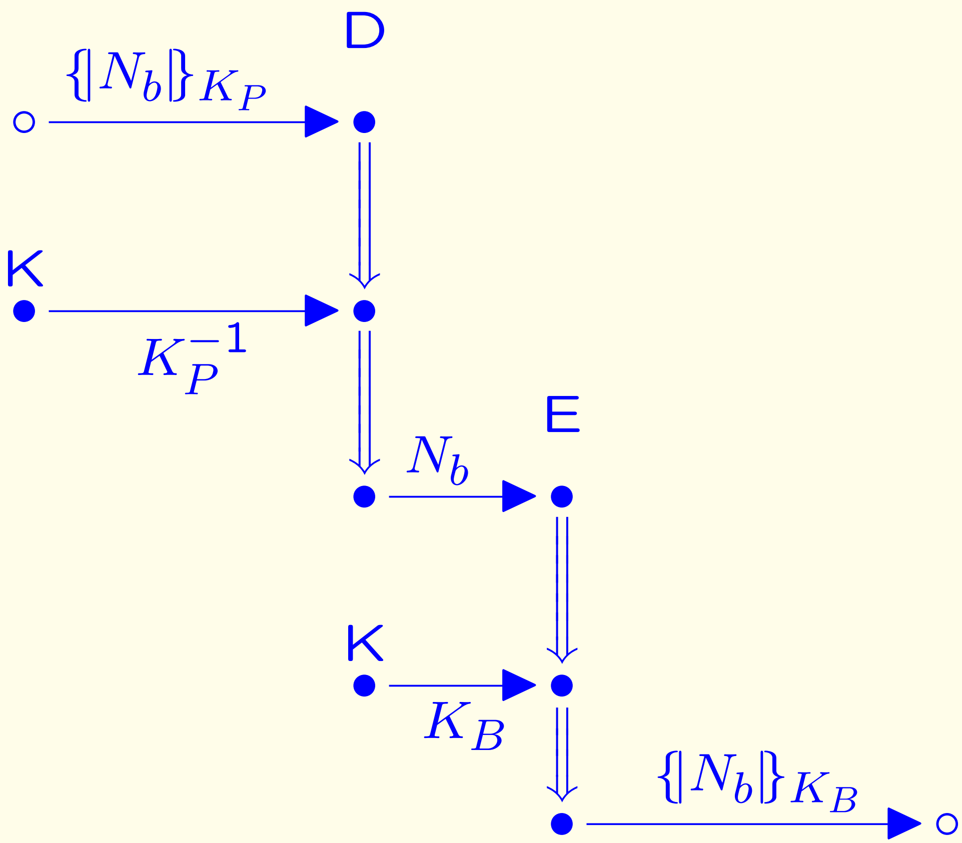


Due to Gavin Lowe (1995)

How the Penetrator Does That, I



How the Penetrator Does That, II



Powers of the Penetrator

- Initiate values
  - Texts (nonces, names, etc.)
  - Keys
    (public, compromised, or invented)
- Construct terms
  - Concatenate given terms
  - Encrypt, given key and plaintext
- Destruct terms
  - Separate concatenated terms
  - Decrypt, given ciphertext and matching decryption key
- Represented as strands

– Sequence of send/receive events by same participant (penetrator in this case)

Strand Spaces

- *Signed term*: a pair $(+, t)$ or $(-, t)$, where t is a term

  $(+, t)$ means transmission of t
  $(-, t)$ means reception of t

- (Σ, tr) is a *strand space* over *A* whenever tr is a mapping from Σ to $(\pm A)^*$

  $s \in \Sigma$ is called a strand

  $s \downarrow i$ is the i^{th} *node*,
  i.e. i^{th} step of s

  $\mathrm{tr}(s)$ is the trace of s,
  i.e. the sequence of its events

- E.g. NS responder: $\mathrm{tr}(s)$ might be

  $-\{\!|N_a\ A|\!\}_{K_B}, \quad +\{\!|N_a\ N_b|\!\}_{K_A}, \quad -\{\!|N_b|\!\}_{K_B}$

First and last terms received
Second term transmitted

Example: NS

- Roles: Initiator, responder;
  Parameters: A, B, N_a, N_b
  - All terms can be checked
  - Uses K_A to mean “The public key of A”
  - List of terms: (signs depend on role)

    $$\{\!|N_a\ A|\!\}_{K_B}, \quad \{\!|N_a\ N_b|\!\}_{K_A}, \quad \{\!|N_b|\!\}_{K_B}$$

  - Values intended to originate uniquely:

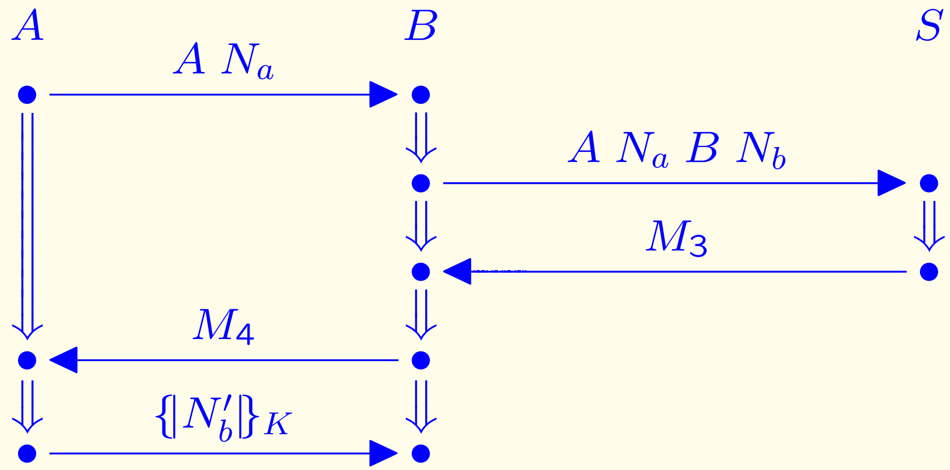
    N_a, N_b
- NSInit$[A, B, N_a, N_b]$:
  set of strands with trace

  $$+\{\!|N_a\ A|\!\}_{K_B}, \quad -\{\!|N_a\ N_b|\!\}_{K_A}, \quad +\{\!|N_b|\!\}_{K_B}$$
- NSLResp$[A, B, N_a, N_b]$:

set of strands with trace

$$-\{\!|N_a\ A|\!\}_{K_B}, \quad +\{\!|N_a\ N_b|\!\}_{K_A}, \quad -\{\!|N_b|\!\}_{K_B}$$

Example: Carlsen, I



$$M_3 = \{\!|K\ N_b\ A|\!\}_{K_B}\ \{\!|N_a\ B\ K|\!\}_{K_A}$$

$$M_4 = \{\!|N_a\ B\ K|\!\}_{K_A}\ \{\!|N_a|\!\}_K\ N_b'$$

Example: Carlsen, II

- Roles: Initiator, responder, server;
  Parameters: A, B, N_a, N_b, K, N_b'
  - B cannot check $\{\!|N_a\ B\ K|\!\}_{K_A}$ part of M_3 (parameter H)
  - Uses K_A to mean "Long term shared key of A"
- Values intended to originate uniquely:
  - Nonces N_a, N_b, N_b'
  - Session key K
- Obligations of key server:
  Avoid session keys
  - Already used previously
  - Equal to long-term key K_A
  - Known initially to penetrator

Achieved probabilistically
Obligation same for all key server protocols

Example: Carlsen, III

- CInit$[A, B, N_a, K, N_b']$:
  set of strands with trace

$$+A\ N_a, \quad -\{\!|N_a\ B\ K|\!\}_{K_A}\ \{\!|N_a|\!\}_K\ N_b', \quad +\{\!|N_b'|\!\}_K$$

- CResp$[A, B, N_a, N_b, K, N_b', H]$:
  set of strands with trace

$$-A\ N_a, \quad +A\ N_a\ B\ N_b, \quad -\{\!|K\ N_b\ A|\!\}_{K_B}\ H,$$

$$+\ H\ \{\!|N_a|\!\}_K\ N_b', \quad -\{\!|N_b'|\!\}_K$$

- CServ$[A, B, N_a, N_b, K]$:
  set of strands with trace

$$-A\ N_a\ B\ N_b, \quad +\{\!|K\ N_b\ A|\!\}_{K_B}\ \{\!|N_a\ B\ K|\!\}_{K_A}$$

Subject to obligations on previous slide

The Goals of Protocols

Strands and Security Goals

- Strand:
  - One principal's experience of one run
- Strand conveys what
  that principal knows directly
  - He sent and received
    a sequence of messages
- Protocol goals concern
  what else has happened
  - Runs of other principals (authentication)
  - Penetrator actions (secrecy)

NS Undesirable Run: Why is this Failure?

- A Needham-Schroeder protocol goal:

  For every B-strand
  (apparently with A),
  there is an A-strand
  (apparently with B),
  and they agree on the nonces N_1, N_2

- The attack shows:

  There can be a B-strand
  apparently with A,
  but no A-strand apparently with B

- Authentication establishes a sound inference:
  - From B's local experience,
    a conclusion about A's behavior follows
- Secrecy of N_a: no strand utters it unencrypted

Epistemology of Protocols

- What can a principal know directly?
  - The send/receive events on its strand
- What can a principal assume reasonably?
  - Penetrator abilities
  - Behaviors of other principals
  - Origination assumptions
- What can a principal infer?
  - Real world must contain events that caused what he saw
  - Message he received was sent by someone
  - Can sometimes infer specific other strands are present
- Bundle definition tailored to model these inferences

Authentication Goals: Example I

- Consider bundle $\mathcal{C}$ in which B undergoes s_r with trace

  $-\{\!|N_a\ A|\!\}_{K_B}, \quad +\{\!|N_a\ N_b|\!\}_{K_A}, \quad -\{\!|N_b|\!\}_{K_B}$

  B knows that s_r is in $\mathcal{C}$

- Responder's guarantee that initiator participated

  If $\mathcal{C}$ contains

  $$s_r \in \mathsf{NSLResp}[A, B, N_a, N_b]$$

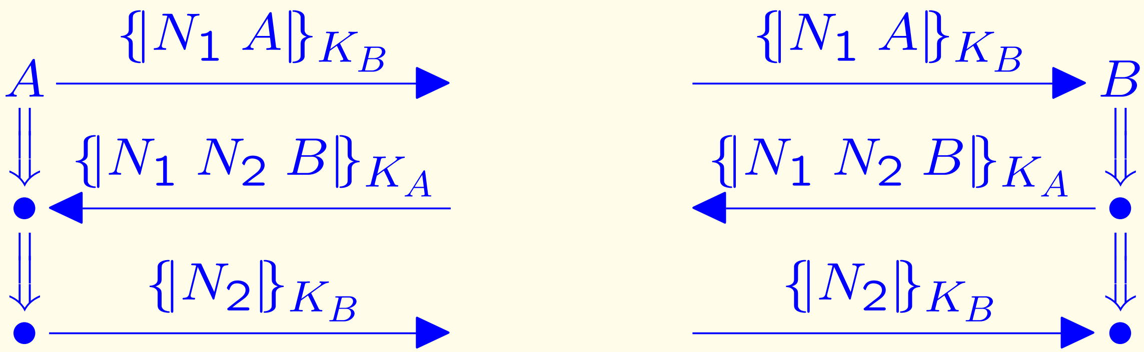
  then $\mathcal{C}$ contains some

  $$s_i \in \mathsf{NSLInit}[A, B, N_a, N_b]$$

  (subject to some origination assumptions)

- This goal is false; counterexample is bundle on slide 14

Needham-Schroeder-Lowe Protocol



Summary of this Introduction

- How crypto protocols fail
- The Dolev-Yao problem
  - Idealize crypto
  - Powerful penetrator
  - Find authentication, confidentiality properties
- Strand spaces
  - Modeling protocols
  - Some definitions
  - Formalizing security goals